DETEKSI ANOMALI PADA LALU LINTAS JARINGAN VICTIM REVERSE TCP DENGAN METODE GRADIENT BOOSTING

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu

Syarat Memperoleh Gelar Sarjana Komputer

OLEH :

VIONA AULIA MEIDY

09011282126075

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

Deteksi Anomali Pada Lalu Lintas Jaringan Victim Reverse TCP Dengan Metode Gradient Boosting

Sebagai salah satu syarat untuk penyelesaian studi

di Program Studi S1 Sistem Komputer

Oleh:

VIONA AULIA MEIDY

09011282126075

Pembimbing 1	**:**	**Prof. Ir. Deris Stiawan, M. T., Ph.D.**
		NIP. 197806172006041002
Pembimbing 2	**:**	**Nurul Afifah, M.Kom.**
		NIP. 199211102023212049

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

SKRIPSI

Anomaly Detection in Victim Reverse TCP Network Traffic Using Gradient Boosting Method

As one of the requirements for completing studies

in the S1 Computer System Study Program

By:

VIONA AULIA MEIDY

09011282126075

Advisor	**1**	**:**	**Prof. Ir. Deris Stiawan, M. T., Ph.D.**
			NIP. 197806172006041002
Advisor	**2**	**:**	**Nurul Afifah, M.Kom.**
			NIP. 199211102023212049

Approved by

Head of Computer Systems Departement

Dr. Ir. Sukemi, M.T

196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 13 Juni 2025

Tim Penguji :

1.	Ketua	:	Dr. Ahmad Zarkasi, M.T.
2.	Penguji	:	Dr. Ir. Ahmad Heryanto, M.T.
3.	Pembimbing 1	:	Prof. Ir. Deris Stiawan, M.T., Ph.D.
4.	Pembimbing 2	:	Nurul Afifah, M.Kom.

Mengetahui, 4/7/25

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

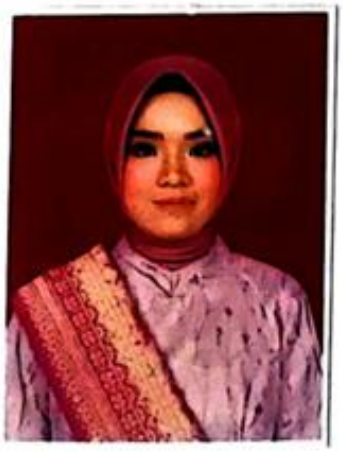
Yang bertanda tangan dibawah ini :

Nama	:	Viona Aulia Meidy
NIM	:	09011282126075
Judul	:	DETEKSI ANOMALI PADA LALU LINTAS JARINGAN VICTIM REVERSE TCP DENGAN METODE GRADIENT BOOSTING

Hasil Pengecekan Software Turnitin : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Juni 2025

Viona Aulia Meidy

NIM. 09011282126075

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur selalu dipanjatkan atas kehadirat Allah SWT yang telah memberikan ridho serta karunia-NYA kepada penulis sehingga dapat menyelesaikan laporan Kerja Praktik dengan judul **"DETEKSI ANOMALI PADA LALU LINTAS JARINGAN VICTIM REVERSE TCP DENGAN METODE GRADIENT BOOSTING"** . sholawat serta salam senantiasa tercurahkan kepada Nabi Muhammad SAW yang telah membawa kedamaian serta Rahmat untuk semesta alam serta dapat menjadi suri teladan bagi umatnya.

Skripsi ini digunakan sebagai salah satu syarat untuk memenuhi sebagian kurikulum dan syarat kelulusan Mata Kuliah Skripsu pada Jurusan Sistem Komputer, Universitas Sriwijaya.

Dalam penyusunan laporan hasil kerja praktek penulis mendapat banyak bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan nikmat jasmani serta rohani sehingga dapat menyelesaikan laporan kerja praktik.
2. Kedua Orang Tua, Keluarga serta teman-teman yang selalu mendoakan serta memberikan motivasi dan semangat.
3. Bapak Prof.Dr.Ir.Erwin, S.Si., M.Si Selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi., M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir.
6. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir.
7. Bapak Dr. Rossi Passarella, M.Eng. selaku Dosen Pembimbing Akademik.
8. Bapak Angga Saputra selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
9. Nabila Sintia dan Ririn Febriana selaku teman seperjuangan yang selalu ada saat susah maupun senang.

10. Teman – teman seperjuangan jurusan sistem komputer angkatan 2021 terkhusus kelas A.
11. Seluruh pihak yang tidak dapat disebutkan satu persatu yang telah memberikan dukungan serta bantuan baik secara moril maupun materil.
12. Almamater.

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung atau pun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Juni 2025

Penulis,

Viona Aulia Meidy

NIM. 09011282126075

DETEKSI ANOMALI PADA LALU LINTAS JARINGAN VICTIM REVERSE TCP DENGAN METODE GRADIENT BOOSTING

Viona Aulia Meidy (09011282126075)

Departement of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email : 09011282126075@student.unsri.ac.id

ABSTRACT

Deteksi anomali pada jaringan merupakan aspek penting dalam keamanan siber. Penelitian ini bertujuan untuk mengevaluasi kinerja model Gradient Boosting dalam mendeteksi anomali pada lalu lintas reverse TCP, serta menginterpretasi hasil deteksi guna membantu analis keamanan memahami pola serangan. Metode yang digunakan dalam penelitian ini mencakup pemrosesan data dengan teknik oversampling untuk menangani ketidakseimbangan kelas, seleksi fitur menggunakan metode Mutual Information, pelatihan model Gradient Boosting, serta evaluasi performa menggunakan confusion matrix dan classification report. Keputusan deteksi diambil berdasarkan analisis dari Wireshark dan Snort. Hasil penelitian menunjukkan bahwa Gradient Boosting memiliki performa yang baik dalam mendeteksi anomali, dengan akurasi sebesar 98,46% setelah dilakukan seleksi fitur menggunakan Mutual Information.

Kata Kunci: Deteksi Anomali, Gradient Boosting, Reverse TCP, Keamanan Jaringan.

ANOMALY DETECTION IN VICTIM REVERSE TCP NETWORK TRAFFIC USING THE GRADIENT BOOSTING METHOD

Viona Aulia Meidy (09011282126075)

Departement of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email : 09011282126075@student.unsri.ac.id

ABSTRACT

Anomaly detection in network traffic is a critical aspect of cybersecurity. This study aims to evaluate the performance of the Gradient Boosting model in detecting anomalies in reverse TCP traffic and to interpret the detection results to assist security analysts in understanding attack patterns. The methodology used in this research includes data preprocessing with oversampling techniques to address class imbalance, feature selection using the Mutual Information method, model training with Gradient Boosting, and performance evaluation using a confusion matrix and classification report. Detection decisions are based on analyses from Wireshark and Snort. The results indicate that Gradient Boosting demonstrates strong performance in detecting anomalies, achieving an accuracy of 98.46% after feature selection with Mutual Information..

Keywods: *Anomaly Detection, Gradient Boosting, Reverse TCP, Network Security*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Malware diperlukan dalam mendeteksi anomali untuk menjaga keamanan sistem. Seiring berjalannya waktu, berdasarkan penelitian [1] malware diperlukan dalam mendeteksi anomali untuk menjaga keamanan sistem. Seiring berjalannya waktu, metode *machine learning* semakin banyak digunakan karena lebih efektif dibandingkan metode berbasis aturan karena kemampuannya yang lebih fleksibel dan adaptif dalam mengenali pola baru serta mendeteksi ancaman yang terus berkembang. Penelitan [2] *Machine learning* dapat digunakan dalam mengambil keputusan yang lebih tepat, karena dapat mempercepat deteksi ancaman yang terus berkembang, selain itu dipilih karena dapat meningkatkan kinerja yang membutuhkan komputansi intensif. Pada penelitan [3] terdapat berbagai macam metode prediksi seperti *neural networks*, akan tetapi dengan menggunakan metode *neural networks* memerlukan GPU (*graphics processing unit*) sehingga prediksi dengan menggunakan teknik berbasis tree-based lebih unggul karena memiliki potensi akurasi yang lebih tinggi.

Penelitian lain [4] menggunakan pemanfaatan model pembelajaran mesin seperti neural network untuk memprediksi tren serangan malware di rantai pasokan siber, hasilnya menunjukkan bahwa neural network memiliki performa terbaik dalam akurasi dan ketepatan prediksi, namun membutuhkan waktu komputasi yang tinggi dan sumber daya yang besar, yang menjadi kendala dalam penerapan skala besar, karena itu pada penelitian [5] sangat penting dirancang IDS *(instruction detection system*), yang efisien dan akurat dan meningkatnya serangan siber dalam beberapa tahun terakhir telah membuat pengembang system untuk mengembangkan deteksi agar memastikan keamanan jaringan dan data.

Metode penelitian [6] dengan *deep learning*, termasuk *Self-Organizing Maps (SOM) dan Long Short-Term Memory (LSTM)*, dapat digunakan dalam mendeteksi anomali, model ini terbukti efektif untuk deteksi dini gangguan, namun memiliki kelemahan berupa kebutuhan data dalam jumlah besar dan waktu komputasi yang

tinggi, hasil menunjukkan bahwa akurasi hybrid LSTM menghasilkan R-Square sebesar 0.9686 dengan nilai RMSE 0.77. Pada penelitian [7] Sistem EDR diadopsi untuk membuat serangan sulit dideteksi, akan tetap system EDR rentan terhadap serangan malware, sehingga diperlukan detector malware ringan, sistem.

Penelitian lain [8] mengusulkan metode deteksi *malware* Teknik *Compact Data Learning* (CDL) dapat digunakan agar dapat mengurangi kompleksitas data serta melakukan pengoptimalan efisiensi pelatihan model tanpa mengorbankan akurasi deteksi, akan tetapi walaupun menghemat waktu pelatihan CDL bergantung pada pemilihan fitur yang relevan, sehingga dapat memengaruhi performa jika pemilihan fitur tidak optimal, akurasi sistem deteksi malware yang menggunakan metode Compact Data Learning (CDL) mencapai hingga 99%.

Penelitian [9] dengan metode LSTM dapat digunakan agar dapat meningkatkan keakuratan deteksi ancaman di lingkungan industri, terutama di sektor energi. Selain itu, terdapat juga metode seperti *CatBoost, LightBoost, dan Xgboost* memiliki tingkat efektif dalam prediksi yang dapat memberikan prediksi yang akurat, namun dengan metode memerlukan sumber daya komputansi tinggi dan memerlukan dataset yang kompleks, akan tetapi metodologi *gradient boosting* memiliki keunggulan dalam meningkatkan keakuratan prediksi secara signifikan [10].

Metode algoritma berbasis *gradient boosting*, pada penelitian [11] akan memberikan pengurangan yang signifikan sehingga dapat menghasilkan hasil prediksi dengan akurasi tinggi dan mengatasi masalah *over-fitting*. Dengan adanya interaksi yang kompleks antara variabel yang berbeda, pada penelitian [12] algoritma *gradient boosting* diperkenalkan agar dapat mempelajari hubungan antara parameter. Metode [13] *gradient boosting* adalah metode pembelajaran dengan teknik *esemble*, yang setiap pada iterasi set pelatihan dipilih secara acak dan diperiksa dari model dasar pada *gradient boosting* dengan koefisien determinasi sebesar 97,20%. Selain itu terdapat metode *gradient tree boosting* pada penelitian [14] yang dikombinasikan dengan principal component analysis yang digunakan dalam prediksi, namun, GTB rentan terhadap *overfitting* pada dataset kecil atau ketika variabel masukan sangat beragam. Pada penelitian [15] telah digunakan

etode proposed analytical akan tetapi tidak memiliki interpretasi tentang parameter yang penting, oleh karena itu digunakan metode *machine learning* dengan *gradient boosting*.

Metode *gradient boosting* dapat diterapkan agar dapat memprediksi parameter *fitting*, sehingga pada penelitian [16] memberikan hasil yang lebih akurat dan konservatif yang membuktikan bahwa metode *gradient boosting* memiliki solusi dalam melakukan pengoptimalan dari analisis kegagalan, selanjutnya agar dapat menunjukan prediksi dengan akurasi yang baik maka diperlukan pembagian set data dengan menggunakan berbagai macam set data *Training* dan *testing* dengan hasil yang akurat dapat diketahui bahwa metode dapat memecahkan permasalahan dalam pendeteksian, karena peningkatan signifikan dalam varian *malware* mengharuskan pengembangan teknik deteksi yang lebih efektif. Pada penelitian [17][18] Model yang diusulkan menggabungkan fitur perilaku dari analisis dinamis dan ekstraksi pola tersembunyi dengan pembelajaran mendalam, sehingga memberikan pendekatan yang komprehensif untuk deteksi *malware* varian yang lebih akurat. Analisis dengan metode machine learning berdasarkan penelitian [19] dapat meningkatkan tujuan dalam meningkatkan keamanan siber, karena itu pada penelitian [20] pendeteksian anomali sangat dibutuhkan terutama dalam konteks keamanan jaringan.

1.2 Rumusan Masalah

1. Bagaimana proses ekstraksi pada dataset jaringan reverse TCP?
2. Bagaimana teknik seleksi fitur yang digunakan agar dapat memilih fitur yang relevan?
3. Bagaimana performa *Gradient Boosting* dalam mendeteksi jaringan *reverse TCP*?

1.3 Batasan Masalah

1. Penelitian hanya akan berfokus pada deteksi anomali pada jaringan reverse TCP menggunakan *Gradient Boosting*, tanpa membahas jenis algoritma *machine learning* lainnya.

2. Data yang digunakan dalam penelitian ini terbatas pada data lalu lintas jaringan *reverse* TCP yang telah ditentukan dan tidak mencakup semua jenis lalu lintas jaringan.
3. Proses evaluasi model dibatasi pada metrik seperti akurasi, precision, recall, F1-score, dan analisis terhadap fitur penting.

1.4 Tujuan:

1. Ekstraksi pada dataset jaringan *reverse* TCP bermanfaat untuk memperoleh data terstruktur dengan fitur-fitur penting guna analisis dan deteksi ancaman.
2. Seleksi fitur yang relevan berguna untuk meningkatkan efisiensi model dengan mengurangi dimensi data, meningkatkan akurasi, dan mengoptimalkan proses deteksi.
3. Evaluasi performa Gradient Boosting membantu menentukan efektivitasnya dalam mendeteksi lalu lintas reverse TCP.

1.5 Manfaat:

1. Pemahaman proses ekstraksi pada dataset jaringan *reverse* TCP diharapkan dapat meningkatkan efektivitas pengolahan data untuk analisis anomali.
2. Penerapan teknik seleksi fitur yang tepat berkontribusi dalam pemilihan fitur yang relevan, sehingga meningkatkan akurasi deteksi anomali.
3. Evaluasi performa *Gradient Boosting* dalam mendeteksi jaringan reverse TCP memberikan wawasan tentang efektivitas algoritma dalam mengidentifikasi ancaman keamanan.

1.6 Metodologi penelitian

Penelitian dapat dilakukan dengan berbagai tahap, yaitu:

1. Tahap pertama (Studi Literatur)

Tahap pertama adalah studi literatur, dilakukan studi pada topik penelitian yang berkaitan dengan judul yang ditempuh, studi litaratur didapat dari jurnal maupun dokumen ilmiah lainnya.

2. Tahap kedua (Topologi dan dataset)

Tahap kedua berkaitan dengan rancangan dari topologi pada dataset *network traffic malware* yang digunakan.

3. Tahap ketiga (Pengolahan Data)

Tahap ketiga adalah melakukan pengolahan dataset reverse TCP dengan format pcap yang kemudian di ekstrak menjadi csv.

4. Tahap keempat (Perancangan Model Deteksi)

Tahap keempat berkaitan dengan perancangan model deteksi, pada tahap keempat model akan dideteksi dengan metode *Gradient Boosting*.

5. Tahap kelima (Pengujian Model Deteksi)

Tahap kelima berkaitan dengan penentuan model terbaik yang akan digunakan sebagai implementasi. , model *Gradient Boosting* dikembangkan untuk mendeteksi anomali dalam jaringan *reverse* TCP. Model dibangun dengan parameter yang telah dioptimalkan untuk meningkatkan akurasi.

6. Tahap Keenam (Hasil dan Analisis)

Hasil evaluasi kinerja model kemudian dianalisis untuk memahami faktor-faktor yang mempengaruhi efektivitas *Gradient Boosting* dalam mendeteksi anomali pada jaringan reverse TCP. Analisis ini juga melibatkan identifikasi pola anomali yang terdeteksi oleh model serta kekuatan dan kelemahan model dalam konteks deteksi anomali jaringan.

7. Tahap ketujuh (Kesimpulan dan Saran)

Pada tahap terakhir, kesimpulan ditarik berdasarkan hasil penelitian, termasuk temuan utama mengenai kinerja *Gradient Boosting* dalam mendeteksi anomali jaringan. Selain itu, saran diberikan untuk pengembangan lebih lanjut, seperti penerapan metode lain atau perbaikan model, untuk meningkatkan akurasi dan menurunkan tingkat *false positives* pada deteksi anomali di jaringan *reverse* TCP.

1.7 Sistematika Penulisan

Sistematika penulisan adalah sebagai berikut:

BAB I PENDAHULUAN

Bab pertama berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah untuk, tujuan serta manfaat yang diharapkan dari dapat bermanfaat untuk kedepannya.

BAB II TINJAUAN PUSTAKA

Bab membahas mengenai teori dari berbagai penelitian terdahulu yang relevan, meliputi konsep dasar deteksi anomali pada jaringan, metode *Gradient Boosting*.

BAB III METODOLOGI PENELITIAN

Bab ketiga menguraikan langkah-langkah penelitian menjadi lebih terperinci, dimulai dari studi literatur yang relevan, melakukan analisis dataset *reverse* TCP, pembuatan topologi serta pembagian data untuk *Training* dan *testing*, pada metode *Gradient Boosting*, evaluasi kinerja model, serta analisis dari berbagai macam faktor yang mempengaruhi akurasi deteksi anomali pada jaringan *reverse* TCP.

BAB IV HASIL DAN ANALISIS

Bab keempat menyajikan hasil penelitian yang diperoleh serta analisis dari hasil yang selesai diteliti, mulai dari akurasi metode *Gradient Boosting* serta tingkat *false positives*.

BAB V KESIMPULAN DAN SARAN

Bab kelima meyajikan kesimpulan yang diambil dari hasil penelitian, termasuk penelitian tentang mengenai kinerja *Gradient Boosting* dalam mendeteksi anomali jaringan *reverse* TCP.

DAFTAR PUSTAKA

[1] W. Gong *et al.*, "Gradient boosting decision tree algorithms for accelerating nanofiltration membrane design and discovery," *Desalination*, vol. 592, no. August, 2024, doi: 10.1016/j.desal.2024.118072.

[2] S. Yalcin Kuzu, "Evaluation of gradient boosting and deep learning algorithms in dimuon production," *J. Mol. Struct.*, vol. 1277, p. 134834, 2023, doi: 10.1016/j.molstruc.2022.134834.

[3] D. Guven and M. O. Kayalica, "Analysing the determinants of the Turkish household electricity consumption using gradient boosting regression tree," *Energy Sustain. Dev.*, vol. 77, no. October, p. 101312, 2023, doi: 10.1016/j.esd.2023.101312.

[4] S. Li, "Comparative Analysis of Predicting Malware Attack Trends in Cyber Supply Chain Using Multiple Classification Models," *IEEE Access*, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3471802.

[5] P. Lavanya, R. P. Singh, U. Kumaran, and P. Kumar, "Gradient Boosting classifier performance evaluation using Generative Adversarial Networks," *Procedia Comput. Sci.*, vol. 235, pp. 3016–3024, 2024, doi: 10.1016/j.procs.2024.04.285.

[6] V. S. B. Rama, S. H. Hur, and J. M. Yang, "Predictive Maintenance and Anomaly Detection of Wind Turbines Based on Bladed Simulator Models," *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 4633–4638, 2023, doi: 10.1016/j.ifacol.2023.10.974.

[7] T. H. Hai, V. Van Thieu, T. T. Duong, H. H. Nguyen, and E. N. Huh, "A Proposed New Endpoint Detection and Response With Image-Based Malware Detection System," *IEEE Access*, vol. 11, no. November, pp. 122859–122875, 2023, doi: 10.1109/ACCESS.2023.3329112.

[8] S. K. Kim, X. Feng, H. Al Hamadi, E. Damiani, C. Y. Yeun, and S. Nandyala, "Advanced Machine Learning Based Malware Detection Systems," *IEEE Access*, vol. 12, no. August, pp. 115296–115305, 2024, doi:

10.1109/ACCESS.2024.3434629.

[9] I. Almomani, T. Almashat, and W. El-Shafai, “Maloid-DS: Labeled Dataset for Android Malware Forensics,” *IEEE Access*, vol. 12, no. May, pp. 73481–73546, 2024, doi: 10.1109/ACCESS.2024.3400211.

[10] R. A. Sobolewski, M. Tchakorom, and R. Couturier, “Gradient boosting-based approach for short- and medium-term wind turbine output power prediction,” *Renew. Energy*, vol. 203, no. December 2022, pp. 142–160, 2023, doi: 10.1016/j.renene.2022.12.040.

[11] N. Aksoy and I. Genc, “Predictive models development using gradient boosting based methods for solar power plants,” *J. Comput. Sci.*, vol. 67, no. January, p. 101958, 2023, doi: 10.1016/j.jocs.2023.101958.

[12] H. Chen, Z. Shen, L. Wang, C. Qi, and Y. Tian, “Prediction of undrained failure envelopes of skirted circular foundations using gradient boosting machine algorithm,” *Ocean Eng.*, vol. 258, no. January, p. 111767, 2022, doi: 10.1016/j.oceaneng.2022.111767.

[13] T. Sripetdee *et al.*, “Extreme gradient boosting machine for modeling hydrogen gas storage in carbon slit pores from molecular simulation data,” *Energy Reports*, vol. 8, pp. 16–21, 2022, doi: 10.1016/j.egyr.2022.10.229.

[14] T. Katongtung, T. Onsree, K. Y. Tippayawong, and N. Tippayawong, “Prediction of biocrude oil yields from hydrothermal liquefaction using a gradient tree boosting machine approach with principal component analysis,” *Energy Reports*, vol. 9, no. S11, pp. 215–222, 2023, doi: 10.1016/j.egyr.2023.08.079.

[15] I. U. Ekanayake, S. Palitha, S. Gamage, D. P. P. Meddage, K. Wijesooriya, and D. Mohotti, “Predicting adhesion strength of micropatterned surfaces using gradient boosting models and explainable artificial intelligence visualizations,” *Mater. Today Commun.*, vol. 36, no. May, p. 106545, 2023, doi: 10.1016/j.mtcomm.2023.106545.

[16] S. Sinha, C. Sankar Rao, A. Kumar, D. Venkata Surya, and T. Basak,

"Exploring and understanding the microwave-assisted pyrolysis of waste lignocellulose biomass using gradient boosting regression machine learning model," *Renew. Energy*, vol. 231, no. January, p. 120968, 2024, doi: 10.1016/j.renene.2024.120968.

[17] A. Sharma and R. Tiwari, "Anomaly detection in smart grid using optimized extreme gradient boosting with SCADA system," *Electr. Power Syst. Res.*, vol. 235, no. February, p. 110876, 2024, doi: 10.1016/j.epsr.2024.110876.

[18] A. A. Al-Hashmi *et al.*, "Deep-Ensemble and Multifaceted Behavioral Malware Variant Detection Model," *IEEE Access*, vol. 10, pp. 42762–42777, 2022, doi: 10.1109/ACCESS.2022.3168794.

[19] D. Agnew, A. Del Aguila, and J. Mcnair, "Enhanced Network Metric Prediction for Machine Learning-Based Cyber Security of a Software-Defined UAV Relay Network," *IEEE Access*, vol. 12, no. March, pp. 54202–54219, 2024, doi: 10.1109/ACCESS.2024.3387728.

[20] A. Lundstrom, M. O'Nils, F. Z. Qureshi, and A. Jantsch, "Improving Deep Learning Based Anomaly Detection on Multivariate Time Series Through Separated Anomaly Scoring," *IEEE Access*, vol. 10, no. September, pp. 108194–108204, 2022, doi: 10.1109/ACCESS.2022.3213038.

[21] A. M. S. Sulaimany, "Android malware detection through centrality analysis of applications network," *Appl. Soft Comput.*, vol. 137, p. 112058, 2024, doi: 10.1016/j.asoc.2024.112058.

[22] J. Jagadeesan, S. Nandhini, and B. Sathiyaprasad, "Classification of malware for security improvement in IoT using heuristic aided adaptive multi-scale and dilated ResneXt with gated recurrent unit," *Appl. Soft Comput.*, vol. 163, no. November 2023, p. 111838, 2024, doi: 10.1016/j.asoc.2024.111838.

[23] F. Zhou, D. Wang, Y. Xiong, K. Sun, and W. Wang, "FAMCF: A few-shot Android malware family classification framework," *Comput. Secur.*, vol. 128, p. 104027, 2024, doi: 10.1016/j.cose.2024.104027.

[24] F. S. Hossain and T. Yuneda, "An exquisitely sensitive variant-conscious

post-silicon Hardware Trojan detection," *Integration*, vol. 93, no. June, 2023, doi: 10.1016/j.vlsi.2023.102064.

[25] A. Sengupta, A. Anshul, and R. Chaurasia, "Exploration of optimal functional Trojan-resistant hardware intellectual property (IP) core designs during high level synthesis," *Microprocess. Microsyst.*, vol. 103, no. October, p. 104973, 2023, doi: 10.1016/j.micpro.2023.104973.

[26] F. N. E. and A. A. Bayrakci, "Delay based hardware Trojan detection exploiting spatial correlations to suppress variations," *Integration*, vol. 89, p. 103006, 2023, doi: 10.1016/j.vlsi.2023.03.006.

[27] L. Shen, M. Fang, and J. Xu, "GHGDroid: Global heterogeneous graph-based android malware detection," *Comput. Secur.*, vol. 141, no. March, p. 103846, 2024, doi: 10.1016/j.cose.2024.103846.

[28] Q. M. Y. H. AlOmari and M. A. Al-Betara, "A Comparative Analysis of Machine Learning Algorithms for Android Malware Detection," *Procedia Comput. Sci.*, vol. 217, pp. 265–272, 2023, doi: 10.1016/j.procs.2023.03.101

[29] S. E. Şahin, E. M. Özyedierler, and A. Tosun, "Predicting vulnerability inducing function versions using node embeddings and graph neural networks," *Inf. Softw. Technol.*, vol. 145, no. December 2021, p. 106822, 2022, doi: 10.1016/j.infsof.2022.106822.

[30] S. K. Shandilya, C. Ganguli, I. Izonin, and P. A. K. Nagar, "Cyber attack evaluation dataset for deep packet inspection and analysis," *Data Br.*, vol. 46, p. 108771, 2023, doi: 10.1016/j.dib.2022.108771.

[31] G. Amponis, T. Lagkas, K. Tsiknas, P. Radoglou-Grammatikis, and P. Sarigiannidis, "Introducing a New TCP Variant for UAV networks following comparative simulations," *Simul. Model. Pract. Theory*, vol. 123, no. December 2022, p. 102708, 2023, doi: 10.1016/j.simpat.2022.102708.

[32] Y. Lu, X. Ma, and C. Cui, "DCCS: A dual congestion control signals based TCP for datacenter networks," *Comput. Networks*, vol. 236, p. 110457, 2024, doi: 10.1016/j.comnet.2024.110457.

[33] M. M. Shafi, A. H. Lashkari, and A. H. Roudsari, “NTLFlowLyzer: Towards generating an intrusion detection dataset and intruders behavior profiling through network and transport layers traffic analysis and pattern extraction,” *Comput. Secur.*, vol. 148, no. November 2023, p. 104160, 2025, doi: 10.1016/j.cose.2024.104160.

[34] M. Sarhan, S. Layeghy, and M. Portmann, “Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-Based Network Intrusion Detection,” *Big Data Res.*, vol. 30, p. 100359, 2022, doi: 10.1016/j.bdr.2022.100359.

[35] S. Adiwal, B. Rajendran, P. S. D., and S. D. Sudarsan, “DNS Intrusion Detection (DID) — A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks,” *Franklin Open*, vol. 2, no. January, p. 100010, 2023, doi: 10.1016/j.fraope.2023.100010.

[36] A. Waleed, A. F. Jamali, and A. Masood, “Which open-source IDS? Snort, Suricata or Zeek,” *Comput. Networks*, vol. 213, no. June, p. 109116, 2022, doi: 10.1016/j.comnet.2022.109116.

[37] S. L. Boye *et al.*, *The design space of visualization tools for data science education: literature review and framework for future designs*, vol. 53. Elsevier B.V., 2023. doi: 10.1016/j.ijcci.2024.100698.

[38] B. Ouadi, A. Khatir, E. Magagnini, M. Mokadem, L. Abualigah, and A. Smerat, “Optimizing silt density index prediction in water treatment systems using pressure-based gradient boosting hybridized with Salp Swarm Algorithm,” *J. Water Process Eng.*, vol. 68, no. October, p. 106479, 2024, doi: 10.1016/j.jwpe.2024.106479.

[39] Q. He, H. Huang, and Y. Wang, “Food Bioscience Detection technologies , and machine learning in food : Recent advances and future trends,” *Food Biosci.*, vol. 62, no. September, p. 105558, 2024, doi: 10.1016/j.fbio.2024.105558.

[40] G. Phillips *et al.*, “Setting nutrient boundaries to protect aquatic communities: The importance of comparing observed and predicted

classifications using measures derived from a confusion matrix," *Sci. Total Environ.*, vol. 912, no. November 2023, 2024, doi: 10.1016/j.scitotenv.2023.168872.

[41] H. Setiawan, *Visualisasi Serangan Trojan Metasploit pada Android dengan Metode K-Means*, Skripsi Sarjana, Jurusan Sistem Komputer, Universitas Sriwijaya, Palembang, 2024. [Online]. Tersedia: https://repository.unsri.ac.id/146546/1/RAMA_56201_09011182025004_0003047905_01_front_ref.pdf